REMARKS

Reconsideration of the present application is respectfully requested. Claims 1-16 and 46-49 were previously canceled. In this amendment, claims 23-32 and 54 have been canceled, and claims 17, 33-38 and 50 have been amended. Therefore, claims 17-22, 33-45, 50-53, 55 and 56 are now pending.

Status of Claims

Claims 17-21, 24-26, 29-35, 41-45, 50-53, 55 and 56 were rejected under 35 U.S.C. § 102(e) as allegedly being anticipated by U.S. Patent no. 6,609,113 of O'Leary et al. ("O'Leary"). Claims 22 and 27 stand rejected under 35 U.S.C. § 103(a) as allegedly being unpatentable based on O'Leary in view of WO 96/13814 of Vazvan. Claims 23, 28, 39 and 40 stand rejected under 35 U.S.C. § 103(a) as allegedly being unpatentable based on O'Leary and Vazvan in view of U.S. Patent no. 6,868,391 of Hultgren ("Hultgren").

Overview of the Invention

Before discussing the differences between the cited art and the present invention, an overview of the invention may be helpful. The present invention provides an innovative modality of credit card payment processing, that can benefit all parties involved in a transaction, particularly when the consumer has a wireless device such as a cell phone and is present at a merchant's place of business. The invention enables a wireless telecommunications network operator ("telecommunications carrier") to validate the identities of credit card users who use wireless devices such as cellular telephones (and who therefore subscribe to the carrier's service), and to ensure that the credit card users approve the transactions and receive receipts for the transactions. In certain embodiments, this is done by providing a commerce platform, which implements certain key operations associated with a credit card transaction involving a

mobile user. The commerce platform is implemented as one or more computers operated by a single business entity, e.g., the telecommunications carrier.

This is a significant and advantageous departure from known prior art methods of validating credit card transactions. The invention is advantageous in that it can help to reduce fraud risk while being capable of implementation using existing communications and computing hardware infrastructure and without the necessity to retrain merchants or consumers to a different payment paradigm.

Discussion of Rejections

Claims 17, 39 and 50

Independent claims 17 and 50 have been amended to incorporate certain limitations from dependent claims 23 and 54, which are now canceled. Claim 17, for example, recites:

> 17. (Currently amended) A method of facilitating a credit card transaction between a consumer using a wireless communication device and a provider of a product or service, the method comprising:
> in a commerce platform implemented as one or more computer systems operated by a single business entity,
> storing personal information of the consumer, including a credit card number of a credit card issued to the consumer;
> receiving information for requesting the transaction from a remote entity;
> sending information on the transaction to the wireless communication device;
> receiving a signal from the wireless communication device indicating acceptance of the transaction;
> receiving a personal identification code from the wireless communication device;
> using the received personal identification code and the stored personal information on the consumer to verify the identity of the consumer;
> **verifying that the wireless communication device is in geographic proximity to the provider**; and
> in response to verifying the identity of the consumer and verifying that the wireless communication device is in geographic proximity to the provider, sending to a remote entity other than said single business entity a transaction request including information on the transaction and the credit card number, for initiation of a transaction approval process.

Note that independent claims 39 and 50 include similar limitations to those emphasized above in claim 17.

The cited references neither discloses nor suggests such a method or a related apparatus, either individually or in combination.

Regarding the limitation, "verifying that the wireless communication device is in geographic proximity to the provider," the Examiner cites the combination of O'Leary/Vazvan/Hultgren. Office Action, p. 17, rejections of claims 23, 28, 39-40. The Examiner acknowledges that O'Leary/Vazvan does not teach this limitation but contends that Hultgren does, and that it would be obvious to combine those teachings. The Examiner contends that the motivation to make this combination would be "to perform a security check that the user of the mobile device is at a merchant in order to reduce fraud associated with transaction from unauthorized users and /or users in unauthorized locations." Id.

Applicants respectfully disagree and submit that the cited combination of Hultgren with O'Leary/Vazvan is improper. O'Leary, the primary reference relied upon, discloses two basic types of transactions that can be done in conjunction with the disclosed technique:

1) an *on-line* transaction using either a mobile browser or a non-mobile browser (i.e., shopping at a "web store")(col. 4, lines 43-47; col. 15, lines 45-51); or
2) a transaction where the consumer is *physically present* at the merchant's place of business, by *using an ATM or card reader* (col. 13, lines 14-18).

Scenario 2) by definition does not involve a wireless communication device; therefore, the claim limitation in question has no relevance to that scenario. Regarding scenario 1), by the very nature of on-line ("web store") transactions, the physical location of the consumer is irrelevant; indeed, the consumer is almost never physically at the merchant's place of business during an on-line transaction of the sort disclosed in O'Leary (i.e., "web store"). Therefore, even

if the consumer uses a wireless communication device for such a transaction, attempting to verify geographic proximity of the mobile device to the merchant's location would normally be futile and absurd.

Indeed, there is no scenario described in O'Leary which would benefit from verifying that a wireless communication device is in geographic proximity to a provider. As such, there can be no motivation to combine the cited teachings of Hultgren (regarding verifying geographic proximity) with O'Leary. Therefore, the rejection of claims 23 and 39 based on O'Leary/Vazvan/Hultgren was improper and should not be applied to claims 17, 39 and 50 as amended.

Applicants respectfully submit, therefore, that claims 17, 39 and 50 and all claims which depend on them are patentable over the cite dart.

Claim 33

Claim 33 as amended recites:

> 33. (Currently amended) A method of facilitating a **credit transaction** between a consumer and a provider of a product or service, the method comprising:
>
> receiving information associated with the credit transaction from a remote terminal operated by the provider;
>
> **determining whether the *credit* transaction involves use of a personal mobile telecommunication device**;
>
> if the **credit** transaction is determined ***not* to involve use of a personal mobile telecommunication device**, then initiating a transaction approval process by transmitting at least a portion of the received information to a clearing network for approval of the transaction;
>
> if the **credit** transaction is determined **to involve use of a personal mobile telecommunication device**, then
>
> transmitting the received information to **a remote validation entity other than the clearing network** over a secure channel, to enable validation of the credit transaction **by the remote validation entity**, and
>
> upon receiving an indication that the credit transaction has been validated by the remote validation entity, initiating a credit transaction approval process by transmitting at least a portion of the information to the clearing network for approval of the credit transaction.

Claim 33 was rejected under 35 U.S.C. § 102(e) as allegedly being anticipated by O'Leary". Office Action, p. 6. However, O'Leary does not disclose or suggest a method such as recited in claim 33, particularly the operations emphasized above.

On pages 26-27 of the Office Action, the Examiner responds to Applicants' previous arguments by stating, "Per the present application, a predetermined transaction type means no credit card is being used and a non-predetermined type means a credit card is being used." That is incorrect; Applicants are unable to determine the basis for this assumption by the Examiner. Indeed, claim 33, even prior to the present amendment, clearly stated that *both* types of transactions (predetermined type and non-predetermined type) are *credit* transactions (see original claim 33's preamble). In any event, claim 33 has been amended to make that more clear.

Further, claim 33 has been amended to recite that one type of transaction is a *credit* transaction which *involves use of a personal mobile telecommunication device*, whereas the other type of transaction is also a *credit* transaction but *does not involve the use of a personal mobile telecommunication device*. The validation process, per claim 33, is handled differently for these two types of transactions. In the former case (i.e., involving use of a personal mobile telecommunication device), a remote validation entity *other than the clearing network* is used to validate the transaction. This limitation (at least) distinguishes the method of claim 33 from the cited prior art and from conventional credit card transactions in general.

O'Leary does not disclose or suggest determining whether a *credit* transaction involves use of a personal mobile telecommunication device and then handling the transaction validation process differently depending on the outcome of that determination, per claim 33. Nor is there any indication in O'Leary as to why this would be desirable. Therefore, claim 33 and all claims which depend in it are patentable over the cited art.

Claim 41

Claim 41 recites:

41. A method of facilitating a credit card transaction between a consumer and a provider of a product or service, the method comprising:

providing a computer-implemented portal, through which the consumer can remotely access a commerce application;

storing personal information of the consumer in a database within a trusted domain, the trusted domain excluding the consumer and the provider, the personal information including a credit card number of a credit card issued to the consumer;

receiving, *from a remote entity within the trusted domain*, information for requesting the transaction, including an amount of the transaction and a provider identifier;

storing the information for requesting the transaction;

generating a session identifier corresponding to the transaction in response to receiving the information for requesting the transaction;

associating the session identifier with the stored information for requesting the transaction;

sending the session identifier to a remote entity, *for subsequent communication to the consumer*;

receiving a confidential personal identification code and **a *user-input* session identifier** from a wireless communication device via a wireless communications network;

using the received personal identification code, the user-input session identifier, and the stored personal information of the consumer **to attempt to validate the transaction**, including

using the personal identification code and the stored personal information to verify the identity of the consumer, and

using the *user-input* session identifier to look up the stored information for requesting the transaction and to associate the consumer with the transaction;

if the transaction is successfully validated, then sending information on the transaction to the wireless communication device over the wireless network, to cause the wireless communication device to output a prompt to accept or decline the transaction;

receiving a signal from the wireless communication device indicating acceptance of the transaction;

in response to receiving the signal indicating acceptance of the transaction, sending to the remote entity a transaction request including information on the transaction and the credit card number, for initiation of a transaction approval process by a clearing network, without sending the credit card information outside the trusted domain;

receiving a signal indicating the transaction has been approved by the clearing network; and

in response to receiving the signal indicating the transaction has been approved by the clearing network,

storing a digital receipt of the transaction in association with the identity of the consumer; and

sending a signal to the wireless communication device over the

wireless communication network to cause the wireless communication device to output a message confirming completion of the transaction. (Emphasis added.)

O'Leary does not disclose or suggest a method such as recited in claim 41, particularly the operations emphasized above in bold. Applicants respectfully maintain their previous arguments regarding claim 41. Applicants respectfully maintain that the Examiner's interpretation of O'Leary is incorrect.

First, O'Leary does not disclose or suggest the limitation, "receiving, from a remote entity within the trusted domain, information for requesting the transaction, including an amount of the transaction and a provider identifier." Applicants argued this in their last response, however the Examiner did not rebut or even acknowledge Applicants' argument on this point.

To reiterate, the Examiner cites O'Leary at column 15, line 66 -column 16, line 1 as allegedly disclosing this limitation (Office Action, p. 16). The cited section discloses that *the merchant site* 255 generates and transmits to the user a bill payment message containing information with respect to the prospective purchase. However, claim 41 requires that the merchant is *outside* the trusted domain ("the trusted domain *excluding* the consumer *and the provider*"). Therefore, the merchant in O'Leary cannot be the "remote entity" in the above-mentioned claim limitation, and the cited section of O'Leary does not satisfy that claim limitation. Nor is this limitation disclosed or suggested elsewhere in O'Leary.

Second, as previously noted, claim 41 recites a *session identifier* input *by a user*, and more specifically:

> receiving a confidential personal identification code and **a *user-input* session identifier** from a wireless communication device via a wireless communications network;
>
> using the received personal identification code, the user-input session identifier, and the stored personal information of the consumer **to attempt to validate the transaction**, including
>
> using the personal identification code and the stored personal information to verify the identity of the consumer, and
>
> **using the *user-input* session identifier to look up the stored information for requesting the transaction and to associate the consumer**

with the transaction; . . .. (Emphasis added.)

O'Leary does not disclose or suggest the emphasized limitations, particularly, a *user-input session identifier*, much less using such an identifier in the specific manner recited in claim 41. The Examiner responds to Applicants' latest arguments on this point by stating (Office Action, pp. 24-25):

> O'Leary specifically discloses where multiple transactions can be incorporated into one identifier, thus a session identifier. Column 16, lines 13-17 discloses where a number of purchases are made and then a consolidated payment message is transferred to the wallet. O'Leary further discloses where the identifier is used to designate the transaction for further reference and wherein history or verification can be conducted using the number (column 11, lines 4-14). As the wallet is being used by the user of the account, the user would enter such a number in order to retrieve such information.

The Examiner's interpretation is incorrect for at least two reasons. First, what O'Leary discloses at column 16, lines 13-17 is *not* multiple transactions being incorporated into one identifier. There O'Leary states:

> In the shopping cart method, after the consumer has selected a number of items to purchase, the merchant site 255 totals the items and transmits a consolidated payment message to the PPP enhanced Wallet 215 in step 2F.

This disclosure is simply referring to an ordinary, *single* transaction (purchase) which, just as in the real ("brick-and-mortar") world, may include multiple items. Just as when one buys multiple items at the supermarket in a single transaction, one may also buy multiple items in an on-line "shopping cart" transaction, and that is all O'Leary refers to in the lines cited by the Examiner.

Further, Applicants again respectfully submit that a *transaction* is not the same as a *session* according to those terms' ordinary meanings, and as such, a transaction identifier is not the same as a session identifier. During electronic commerce, more than one transaction can be performed during a particular session. Therefore, O'Leary's disclosure of transaction identifiers also is no suggestion of a session identifier, much less a user input session identifier

being used in the particular manner recited in claim 41 (see limitations emphasized above in bold). Even if the transaction identifiers disclosed in O'Leary were considered to be session identifiers, they are not input *by a user* per claim 41 nor used in the manner recited in claim 41.

The Examiner's response regarding the "user-input" aspect of the recited session identifier is quoted above and is also incorrect. Implicit in the clear language of claim 41 is the requirement that the session identifier has *already been input by the user* when it is used to validate the transaction (otherwise, the modifier "user-input" in the claim limitation "using the . . . *user-input* session identifier . . . to attempt to validate the transaction" would make no sense). This is in contrast with the Examiner's characterization of O'Leary (quoted above), where the Examiner states, "[T]he identifier is used to designate the transaction for further reference and wherein history or verification can be conducted using the number (column 11, lines 4-14). As the wallet is being used by the user of the account, *the user would enter such a number in order to retrieve such information*." Office Action, p. 25 (emphasis added). The identifier in O'Leary referred to by the Examiner may be input by the user at some point *after it has been generated by the system*, but it is *not* a *user-input* session identifier *at the time it is used to validate a transaction* per claim 41 (assuming it is used to validate a transaction at all). O'Leary does not disclose or suggest any session identifier which has been input by a user being used to validate a transaction.

Therefore, claim 41 and all claims which depend on it are patentable over the cited art for at least these reasons.

Conclusion

For the foregoing reasons, the present application is believed to be in condition for allowance, and such action is earnestly requested.

If there are any additional charges, please charge Deposit Account No. 02-2666.

Respectfully submitted,

BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN LLP

Dated: 12/28/2006

Jordan M. Becker
Reg. No. 39,602

Customer No. 26529
12400 Wilshire Blvd.
Seventh Floor
Los Angeles, CA 90025
(408) 720-8300